UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/754,652 | 01/04/2001 | Susumu Kusakabe | 112857-228 | 2981 |

29175 7590 03/01/2006

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

| EXAMINER | |
|---|---|
| SIMITOSKI, MICHAEL J | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

DATE MAILED: 03/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/754,652 | KUSAKABE ET AL. | |
| | Examiner | Art Unit | |
| | Michael J. Simitoski | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,5-15 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-15 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. The response of 12/7/2005 was received and considered.

2. Claims 1-2, 5-15 & 17 are pending.

### *Response to Arguments*

3. Applicant's arguments with respect to claims 1-2, 5-15 & 17 have been considered but are moot in view of the new ground(s) of rejection.

4. Applicant's response overcomes the previous objections to and §112 rejections of the claims.

5. Applicant's response (pp. 9-11) argues that the references do not teach or suggest the step of creating file registry information that is created by encrypting memory space specifying information, wherein the file registry information includes the memory space specifying information in an unencrypted condition. However, as described below, this limitation is unclear because it is unclear how, if the file registry information is creating by encrypting memory space specifying information, the file registry information could include the memory space specifying information in an unencrypted condition. The limitation could be read to mean that the memory space specifying information in the file registry information is ultimately stored in an unencrypted condition. In light of this interpretation, applicant is directed to Zuk's teaching of securely transferring the data to the card by encrypting the file registry information, transmitting it and then decrypting it again (Zuk, col. 2, lines 15-27 & col. 5, lines 8-23). In this situation, the file registry information is created by encrypting the memory space specifying information, but ultimately stored in an unencrypted condition.

6. Applicant's response (p. 12) argues that Canetti teaches away from encrypting an update issuer key with the issuer key because the approach is insecure. However, methods of key exchange under certain circumstances are insecure since a key is being transported; however, the method disclosed by Canetti, if the current key is not compromised, is secure. Further, even if the method disclosed by Canetti could, in the right circumstances, be insecure, the method's utility and therefore motivation (to update a key) still stands. Canetti discloses a well-known method of key updating where the current key is used to encrypt a new key. This method requires no extra processing, whereas a method such as using a public key pair to exchange a new key would require the pre-establishment of a second key (public/private key pair). Therefore, one of ordinary skill would have been motivated to encrypt a new key with the current key for the purpose of updating a new key, as taught by Canetti.

### *Claim Rejections - 35 USC § 112*

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-2, 5-15 & 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims are treated as best understood.

Regarding claims 1, 2, 7 & 14, it is unclear how, if the file registry information is creating by encrypting memory space specifying information, the file registry information could include the memory space specifying information in an unencrypted condition.

Regarding claims 1, 2, 7 & 14, the limitation "wherein said management sector is adapted to create said access key information for each of the business organizations by encrypting based on said file key information and said user key information, wherein ..." (last section) is unclear because there is nothing being encrypted "based on said file key information ...".

### *Claim Rejections - 35 USC § 103*

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-2, 7-8, 11 & 14, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 4,710,613 to **Shigenaga** in view of 4,849,614 to Watanabe et al. (**Watanabe**), U.S. Patent 5,161,256 to **Iijima**, U.S. Patent 5,745,571 to **Zuk** and U.S. Patent 5,590,038 to **Pitroda**. Shigenaga discloses an access apparatus possessed by a business organization for accessing a portable electronic device, said access apparatus including means for executing an authentication/identification between the business organization and the portable electronic device/IC card by using a access key information/encrypted random number (col. 9, lines 1-12) and a management center adapted to create said access key information/encrypted random number by encrypting based on said file key information/MPUK and said issuer key information (col. 9, lines 1-12). Shigenaga's system encrypts data between the terminal and the IC card with issuer key information/IPUK (col. 9, lines 1-12). Shigenaga lacks a plurality of business organizations. However, Watanabe teaches a system that allows a common area

accessible to any enterprise and certain areas to be accessed only from the pertinent enterprise (col. 2, lines 11-14). Watanabe's system stores multiple areas on the card (Fig. 1) each with their own index area (Fig. 1 & Fig. 3); the index areas describing which keys area required to identify an enterprise for access to that specific area of the card (Fig. 3, 3rd and 4th bytes & col. 7, lines 1-46), wherein the keys consist of one or more of an enterprise key, an issuer key, a personal key and a control key (col. 7, lines 10-23). The keys are read into the card and compared with stored values (col. 5, lines 15-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the encrypted random number/access key information of Shigenaga to access an area corresponding to the file key information/MPUK/enterprise key. One of ordinary skill in the art would have been motivated to perform such a modification to allow multiple enterprises to access the same card securely and privately by submitting a key to the card, as taught by Watanabe (col. 2, lines 11-14, col. 5, lines 15-35, col. 7, lines 1-46, Fig. 1 & Fig. 3, 3rd and 4th bytes). As modified, Shigenaga lacks means for transmitting file registry information and a management sector, described in the claims. However, Iijima teaches that to send a file to an IC card that has a plurality of areas to be accessed by different applications (col. 1, lines 10-25), an input command in the form of a data file definition command (file registry information) is sent and memory is allocated based on the size specified in the command (col. 4, lines 38-59& Fig. 11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shigenaga to include means for transmitting file registry information to said portable device/IC card and to include a management sector to generate file registry information, and because Shigenaga transfers data to the card encrypted with the issuer key information/IPUK, to generate

the registry information based on the issuer key information, to create said file registry information by securing memory space in the portable electronic device, said memory space including memory space specifying information. One of ordinary skill in the art would have been motivated to perform such a modification to allocate memory space to an IC card to add data, as taught by Iijima (col. 1, lines 10-25, col. 4, lines 38-59& Fig. 11). As modified, Shigenaga lacks the management sector being adapted to create file key information for each of the business organizations by encrypting said memory space specifying information and said file key information with said issuer key information. However, Zuk teaches that to securely transfer data/key to a card, it is known to encrypt the data, transfer the data from a source and at the card, decrypt the data and store it in memory (col. 2, lines 15-27 & col. 5, lines 8-23). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the file registry information (data file definition/memory space specifying information) and file key information (key required for access). One of ordinary skill in the art would have been motivated to perform such a modification to securely transfer the data to the card, as taught by Zuk (col. 2, lines 15-27 & col. 5, lines 8-23). As modified, Shigenaga lacks performing the encryption with specifically the issuer key. However, Shigenaga discloses requiring an issuer key to access the data (requiring the accessor be the issuer in order to gain access) (col. 7, lines 10-22). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the file registry information and file key information with specifically the issuer key. One of ordinary skill in the art would have been motivated to perform such a modification to send (and encode) and receive (decode) the file key information and file registry information securely (as taught by Zuk) from the issuer (as taught

by Shigenaga). Shigenaga, as modified above, lacks explicitly a plurality of access apparatuses where each of said plurality of business organizations is associated with at least one of said plurality of apparatuses, wherein each of the plurality of access apparatuses are operable to access said portable electronic device. However, Pitroda teaches that universal electronic transaction cards are useful because a plurality of organizations can be accessed with them (col. 2, lines 44-66) through a plurality of point of transactions systems (col. 5, lines 14-24). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shigenaga's system to include a plurality of access apparatuses where each of said plurality of business organizations is associated with at least one of said plurality of apparatuses, wherein each of the plurality of access apparatuses are operable to access said portable electronic device. One of ordinary skill in the art would have been motivated to perform such a modification to access a plurality of different organizations, as taught by Pitroda (col. 2, lines 44-66 & col. 5, lines 14-24).

11. Claims 5, 10, 15 & 17, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shigenaga**, **Watanabe**, **Iijima**, **Zuk** & **Pitroda**, as applied to claims 1, 7 & 14 above, in further view of "SMuG.0" by Canetti et al. (**Canetti**). Shigenaga discloses a system, as described above, but lacks replacing/updating the key as described in claim 15. However, Canetti teaches that one known way to distribute an updated key is to encrypt the new key with the old key (page 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to updated the issuer key information by transmitting issuer key change information generated by encrypting issuer key information/new key with said

issuer key information/old key. One of ordinary skill in the art would have been motivated to perform such a modification to distribute an updated key, as taught by Canetti (page 5).

12. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shigenaga, Watanabe, Iijima, Zuk & Pitroda**, as applied to claim 7 above, in view of U.S. Patent 5,991,749 to Morrill, Jr. (**Morrill**). Shigenaga, as modified above, lacks specifically the portable electronic device being a cellular phone. However, Morrill teaches that cellular phones can be used to perform functions comparable to smart cards to achieve greater security over previous cell phone techniques (col. 1, lines 14-23 & col. 6, lines 16-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable a cellular phone with the features of Shigenaga. One of ordinary skill in the art would have been motivated to perform such a modification to achieve greater security for transactions than previous cellular phones offer, as taught by Morrill (col. 1, lines 14-23 & col. 6, lines 16-35).

***Conclusion***

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
**Or faxed to:**
(571) 273-8300
(for formal communications intended for entry)
**Or:**
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
February 16, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100